7:59 AM PDT 2023-03-29

**Call to Order:** 0803

**Meeting Lead:** Joshua BRICKMAN

**Attendees:** 19

**Member Count:** 70

**Next Meeting:** Wednesday April 5th, 2023

**Highlights:**

~

**Old Business:**

~

**New Business:**

* Reviewed Issue #35 Bare Metal vs multi-tenant issue from previous meeting.
  + Added additional comments to the issue for clarity.
    - *“Based on the TOE’s being evaluated, the need to test on bare metal will be generally obvious. Multi-Tenant is prevalent generally in use by customers and will likely be the vast majority of use cases for evaluations.”*
  + Tom Benkart raised an issue on the potential for multi-tenancy in apps/applications (eg. Vendors that provide security as a service and leverage SIEM apps which operate based on a multi-tenant bases, much like a DBMS.
    - Discussion around modifying the definition for Multi-Tenant to include the following:
      * *“Multi-Tenant refers to cloud services not application functionality”*
    - Roger raised a point on whether this definition is to be used project wide or just for this section. It was identified that we currently do not have a definition for ‘Bare Metal’ in the Guidance Doc.
    - The following definition for ‘Bare Metal’ was added into the Guidance document:
      * *“ A bare-metal server is a physical computer server that is used by one consumer, or tenant, only. Each server offered for rental is a distinct physical piece of hardware that is a functional server on its own.”*
    - The following definition for ‘Multi-Tenant’ was also added to the guidance doc:
      * *“Multi-Tenant uses a shared infrastructure to provide services for multiple cloud customers. Multi-Tenancy means that multiple customers of a cloud vendor are using the same computing resources. Despite the fact that they share resources, cloud customers are logically separated from each other, and their data is isolated.”*
  + Josh shared a discussion (issue #79) item posted by Elaine N regarding the need to limit multi-tenancy as outlined in DoD SRG IL5.
    - Section 5.2.2.3 Impact Level 5 Location and Separation Requirements states the following:
      * *“Virtual/logical separation between DoD and federal Government tenants/missions is sufficient. Virtual/Logical separation between tenant/mission systems is minimally required. Physical separation from non-DoD/non-federal government tenants (ie. Public, local/state government tenants) is required.”*
      * This relates to issue #35. This is a deployment issue and most likely not a CC testing concern although the labs should ask the vendor for their deployment scenarios. Of note, the pricing differential for Bare Metal vs Multi-Tenancy is significant.
    - Alicia Squires shared an example of the cost of bare-metal vs multi-tenant environments. A single bare metal host would cost several thousand dollars per month vs a few hundred for multi-tenant instances.
  + A new section was added to the Guidance document – **“Guidance for Establishing Test Environments on Cloud Infrastructure”**
    - *“As Common Criteria testing requires unique test environments for each TOE that are isolated to prevent contamination of test results, testing on Public Cloud infrastructure raises some initial concerns.*

*In general, the necessity to abstract from underlying hardware layers is dictated by the TOE type in Protection Profiles. For instance, the cPP for Application Software relies only on the underlying OS and makes no distinction on whether that OS is virtualized or not. In this scenario bare metal isolation in the cloud testing would be unnecessary and a multi-tenancy environment is acceptable.*

*A CC lab should be prepared to create and offer cloud testing infrastructure to TOE developers.”*

**Questions/Follow-ups:**

**~**

***End of Meeting – Adjourned 0858 PDT***